CLAIMS

What is claimed is:

1. A system of digital data encryption in a digital device, comprising:

an encryption key generator;

a data buffer; and

a memory controller that directs digital data to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register.

2. The system of claim 1, where the key generator includes:

a clock;

a key store; and

a linear feedback shift register that generates a pseudorandom bit pattern while the linear feedback shift register is enabled and stores a plurality of bits as at least one key in the key store.

3. The system of claim 2, where the pseudorandom bit pattern further includes a random number generator that receives the pseudorandom bit pattern from the linear feedback shift register and provides a random number for use by the digital device.

4. The system of claim 2, where the encryption key generator further includes:

pseudorandom bit pattern generator that creates a bit stream; and

a key store that stores portions of pseudorandom bit pattern as keys.

5. The system of claim 4, including a pseudo random number generator that selects a portion of the pseudorandom bit pattern to be a random number.

6. The system of claim 1, including:

a data mixer that mixes the bits of a byte of the digital data; and

a combiner that combines the byte with a key.

7. The system of claim 1, including:

a sub-key generator that creates a sub-key based on data from the memory controller and the key; and

a combiner that combines the sub-key with the digital data.

8. The system of claim 7, including:

a data mixer that mixes the bits of a byte of digital data; and

a combiner that combines the byte with the sub-key.

9. A system able to decrypt encrypted digital data in a digital device, comprising:

a memory controller that generates a memory request to retrieve encrypted digital data; and

an encryption circuit with a plurality of keys decrypts the encrypted digital data in response to the memory request of the memory controller.

10. The system of claim 9, including a combiner that combines one of the keys with a bank and row information contained in the memory request that results in a sub-key.

11. The system of claim 10, including a data mixer that unmixes bits within a byte after the sub-key is applied to the encrypted digital data.

12. A method of digital data encryption in a digital device, comprising:

generating at least one key;

placing the digital data in a data buffer; and

encrypting the digital data using the at least one key while the digital data is being placed in a rewritable memory.

13. The method of claim 12, where the generating a key includes:

generation of a clock signal;

creating a pseudorandom bit pattern; and

storing at least one portion of the pseudorandom bit pattern in a key store as a key.

14. The method of claim 12, where the pseudorandom bit pattern us generated by a linear feedback shift register.

15. The method of claim 13, includes generating a random number from the pseudorandom bit pattern.

16. The system of claim 12, where the encryption key generator further includes:

a pseudo random bit generator that creates a pseudorandom bit pattern; and

a key store that stores portions of the bit stream as keys.

17. The system of claim 16, including selecting a portion of the pseudorandom bit pattern to be a random number.

18. The method of claim 12, including:

mixing the bits of a byte of the digital data with in a data; and

combining the byte with the key.

19. The method of claim 12, including:

generating a sub-key with data from the memory controller and the key; and

combining the sub-key with the digital data.

20. The method of claim 19, including:

mixing the bits of a byte of digital data with a data mixer; and

combining the byte with the sub-key.

21. The method of claim 12, including generating a random number from the pseudorandom bit pattern.

22. A method to decrypt encrypted digital data in a digital device, comprising:

generating a memory request to retrieve encrypted digital data; and

decrypting the encrypted digital data using at least one key.

23. The method of claim 22, including combining the at least one key with a bank and row information contained in the memory request to generate a sub-key.

24. The method of claim 23, including unmixing a byte of encrypted digital data with a data mixer.

25. A set-top box apparatus in receipt of digital data for storage in a rewritable memory, comprising:

an encryption circuit with at least one key;

a data buffer filled with digital data; and

a memory controller that directs the stores the digital data in the rewritable memory with the digital data being encrypted by the encryption circuit and the at least one key after the digital data has entered the data buffer but prior to being stored in the rewritable memory.

26. The set-top box apparatus of claim 25, where the encryption circuit further includes:

a pseudorandom bit stream generator that creates a pseudorandom bit stream; and

a key store that stores the at least one key that is selected from the pseudorandom bit stream.

27. The set-top box apparatus of claim 25, where the encryption circuit further includes:

a data mixer that mixes the bits of a byte of digital data; and

a combiner that combines the byte with the at least one key.